REMARKS

Claims 1-19 remain in the application. Claims 13-19 are newly added but do not contain any new matter.

The present invention results from a discovery in the field of transmission of secured data that by utilizing a plurality of paths in parallel with each other, with each of the plurality of paths connected to a different one of a plurality of keys for encryption or decryption, throughput of the data that needs to be encrypted or decrypted can be improved.

The Office Action rejected Claims 1, 10, 11, and 12 under 35 U.S.C. §112 as being indefinite because the term "and/or" is indefinite. Applicant has amended Claims 1, 10, 11, and 12 to overcome the rejection and respectfully requests that the rejection be withdrawn.

The Office Action rejected Claims 1, 2, 10, and 12 under 35 U.S.C. §103 as being unpatentable over Admitted Prior Art in view of *Yamamoto et al.* (U.S. 6,307,940, hereinafter "*Yamamoto*").

The present invention seeks to solve a problem in a parallel stream operation apparatus that avoids any complicated key selection operation and improves throughput of encryption and decryption of stream data that is input in parallel. (Spec., Pg. 5, lns. 7-11). It accomplishes this by utilizing a plurality of paths, each corresponding to a different one of a plurality of keys to be used for one of encrypting and decrypting data streams. (Spec., Pg. 5, lns. 12-15; Fig. 2). Input interfaces 101 – 105 can be connected to an antenna, an external apparatus, a CATV circuit, and a public circuit network. When one of the input interfaces 101-105 receives a data stream, the input interface notifies a stream analysis unit 110 of the input stream data, and directs the stream data to the input stream processing unit 121 in response to an output instruction from the stream

control unit 111. (Spec. Pg. 13, lns. 6-12; Fig. 2). The data stream can include, for example, at least video data and audio data.

Furthermore, a control unit of a TV reception apparatus (not shown) notifies the stream analysis unit 110 of a packet identifier (PID) of the transport stream being input into interfaces 101-105 and sets a decryption key for decrypting the encrypted program with the keys 131, 132, 133, and/or 134. The control unit also instructs the stream control unit 111 to have the data from the input interface 101-105 output to the appropriate paths 141-144. The control unit instructs the stream control unit 111 to have the decrypted data in the output stream processing unit 171 from the paths 141-144 to the appropriate output interfaces 181-185. (Spec., pg. 14, lns. 3-22; Fig. 2).

Admitted Prior Art seeks to solve a problem of a parallel stream operation apparatus in a TV reception apparatus. (Spec. pg. 2, lns. 3-5). Data streams enter from input interfaces 1601 – 1605 and are sent to stream processing unit 1621 and subsequently to operation unit 1661. The encrypted streams are decrypted by operation unit 1661 and outputted to the outputs 1681-1685. (Spec. pg. 2, lns. 7-19; Fig. 1). For each packet of the data streams from the input interface 1601-1605, the transfer mediation unit 1651 instructs the selector 1635 to notify the operation unit 1661 of the appropriate decryption key selected from keys 1631-1634. (Pg. 3, ln. 19 – Pg. 4, ln. 14).

The Office Action acknowledges that Admitted Prior Art does not teach or suggest "a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams."

The Admitted Prior Art also does not teach or suggest "an input stream processing unit receiving a plurality of data streams in parallel, and outputting each data stream to the one of the

paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream." As can be seen, the Admitted Prior Art sends data from Stream processing unit 1621 to operation unit 1661. The selector 1635 then selects the appropriate key from key 1631, 1632, 1633, and 1634. Thus, there is only one transportation path between the stream processing unit 1621 and the operation unit 1661.

In contrast, in the present invention, there are keys that correspond to individual paths. For example, in Figure 2 of the present invention, path 141 corresponds with key 131, and path 142 corresponds with key 132, path 143 corresponds with key 133, and path 144 corresponds with key 144. (Spec. pg. 12, ln. 24 – pg. 13, ln. 3).

The cited *Yamamoto* reference seeks to solve a problem of creating "a cryptosystem for an open-algorithm common key block cipher, in which the encryption key for the block cipher is sequentially updated in order to improve safety." (Col. 1, lns. 11-20). It periodically updates block cipher keys with cryptographically secure pseudo-random numbers, in which the block cipher key is updated each time the pseudo-random number generating device outputs $j = k/m$ bits of pseudo-random numbers with regard to the block key length k. This operation purportedly shortens the updating cycle and improves safety. (Col. 9, lns. 33-39).

Yamamoto does not teach or suggest "a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams." The Office Action cited key stream 18 in Figures 5 and 6 as the plurality of paths. However, key stream 18 only transmits bits b_v from shift register 12-1 to DES encrypting device 30 in parallel. Bits b_v are the individual bits that comprise a single key. Thus, key stream 18 is a path for portions of a single key in parallel and not multiple keys. Key stream 18 is not a plurality of paths with each path corresponding to a different one of a plurality of keys.

In contrast, as can be seen in Figure 2 of the present invention, each path 141-144 has a fully operational key 131-134 that corresponds with it, e.g. key 131 corresponds with path 141, key 132 corresponds with path 142, key 133 corresponds with path 143, key 134 corresponds with path 144.

Yamamoto also does not teach or suggest "an input stream processing unit receiving a plurality of data streams in parallel, and outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream." *Yamamoto* does not teach a plurality of keys corresponding with a plurality of paths. Thus, it does not teach or suggest an input stream processing unit operable to receive a plurality of data streams in parallel and output each data stream to the one of the paths that corresponds to a key.

There is also no motivation to combine the Admitted Prior Art with *Yamamoto*. An inventor seeking to solve the problem of a parallel stream operation apparatus in a TV reception apparatus would not look to an invention that seeks to solve the problem of creating "a cryptosystem for an open-algorithm common key block cipher, in which the encryption key for the block cipher is sequentially updated in order to improve safety" for inspiration.

Furthermore, even if the inventions were combined, however improperly, the resulting hypothetical combination would still be deficient with respect to the present invention. The hypothetical combination would not have "a plurality of paths, each corresponding to a different one of a plurality of keys used for encrypting and decrypting data streams," or "an input stream processing unit receiving a plurality of data streams in parallel, and outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream."

As set forth in *In re Kahn*, 441 F.3d 977, 987-988 (Fed. Cir. 2006):

> The motivation-suggestion-teaching test picks up where the analogous art test leaves off and informs the *Graham* analysis. [*Graham v. John Deere Co.*, 383 U.S. 1, 13-14 (1966).]
>
> To reach a non-hindsight driven conclusion as to whether a person having ordinary skill in the art at the time of the invention would have viewed the subject matter as a whole to have been obvious in view of multiple references, the Board must provide some rationale, articulation, or reasoned basis to explain why the conclusion of obviousness is correct. The requirement of such an explanation is consistent with governing obviousness law. . . .
>
> * * *
>
> A suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as "the teaching, motivation, or suggestion may be implicit from the prior art as a whole, rather than expressly stated in the references. . . . The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art." However, rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be *some* articulated reasoning with *some* rational underpinning to support the legal conclusion of obviousness. This requirement is as much rooted in the Administrative Procedure Act [for our review of Board determinations], which ensures due process and non-arbitrary decisionmaking, as it is in §103.

Thus, Claim 1 has novelty and inventiveness over Admitted Prior Art in view of *Yamamoto*.

With respect to Claims 10 and 11, the same arguments for patentability for Claim 1 are also applicable and incorporated herein. Thus, Claims 10 and 11 also have novelty and inventiveness over Admitted Prior Art in view of *Yamamoto*.

With respect to Claim 12, all the arguments for patentability for Claim 1 are again repeated and incorporated herein.

Unlike the present invention, *Yamamoto* is not directed towards a "television reception apparatus" but rather a cryptosystem. Thus, there is no motivation to combine the two references because an inventor seeking to solve the problem of a parallel stream operation apparatus in a TV reception apparatus would not look to an invention that seeks to solve the problem of creating "a cryptosystem for an open-algorithm common key block cipher, in which the encryption key for the block cipher is sequentially updated in order to improve safety" to create a "television reception apparatus."

Furthermore, even if the inventions were combined hypothetically, the resulting hypothetical combination would still be deficient with respect to the present invention. The hypothetical combination would not have "a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams," or "an input stream processing unit receiving a plurality of data streams in parallel, and outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream." Thus, Claim 12 has novelty and inventiveness over Admitted Prior Art in view of *Yamamoto*.

The Office Action rejected Claims 3-7 under 35 U.S.C. §103(a) as being unpatentable over Admitted Prior Art in view of *Yamamoto* and *Baxter III* (U.S. Patent 6,865,643, hereinafter "*Baxter*").

Baxter seeks to solve a problem of a storage processor suited to RAID systems for providing a high throughput for an application such as streaming video data. (Abstract). It accomplishes this by utilizing an application specific integrated chip (ASIC) which supports a store and forward data transfer regime in that host to disk transfers are made by placing a data in storage processor memory under the control of the storage processor, operated on by the ASIC,

and sent to the disk array. (Col. 3, lns. 1-9). The disk to host transfer are made by placing the same data store, checked or regenerated by the ASIC, and sent to the requesting host. (Col. 3, lns. 9-11).

With respect to Claim 5, the Office Action admits that Admitted Prior Art does not teach or suggest "wherein the input stream processing unit outputs one of the data streams to two of the paths, and one of the two paths is connected to the operation unit, and the other of the two paths is directly connected to the output stream processing unit."

The Office Action also admits that Baxter does not teach or suggest "wherein the input stream processing unit outputs one of the data streams to two of the paths, and one of the two paths is connected to the operation unit, and the other of the two paths is directly connected to the output stream processing unit."

Furthermore, *Yamamoto* does not teach or suggest "wherein the input stream processing unit outputs one of the data streams to two of the paths, and one of the two paths is connected to the operation unit, and the other of the two paths is directly connected to the output stream processing unit." In *Yamamoto*, the 17-bit address of ROM_i is inputted from the combination of the 8 bits of c_{vi} and the 9 bits of b_{v+1} as shown in Figure 7. Thus, two bit sources are combined to form a single address.

In contrast, in Figure 13 of the present invention, the input stream control unit 1201 outputs one of the data streams to both path 1211 which goes towards the operation unit 161 and branch path 1221 which goes to the output stream processing unit. Branch paths 1221 to 1224 branch from the paths 1211 to 1214. (Pg. 33, lns. 13-16). Thus, the input stream processing unit outputs one of the data streams to two paths as opposed to combining two bit sources to form a

single address. Thus, Claim 5 is novelty over the Admitted Prior Art in view of *Yamamoto* and *Baxter*.

With respect to Claim 13, Admitted Prior Art does not teach or suggest "wherein the input stream processing unit converts the plurality of data streams to a format that is useable as content data before outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream." The Admitted Prior Art does not specify that it converts the data streams to a format that is useable as content data.

Yamamoto also does not teach or suggest "wherein the input stream processing unit converts the plurality of data streams to a format that is useable as content data before outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream." *Yamamoto* does not contemplate converting the content data before outputting each data stream, much less converting the content data to format useable as content data.

Baxter also does not teach or suggest "wherein the input stream processing unit converts the plurality of data streams to a format that is useable as content data before outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream." *Baxter* does not contemplate converting the content data before outputting each data stream, much less converting the content data to format useable as content data.

Thus, Claim 13 has novelty and inventiveness over the Admitted Prior Art, *Yamamoto*, and *Baxter*.

With respect to Claim 14, Admitted Prior Art does not teach or suggest "wherein the input stream processing unit converts the plurality of data streams to a packetized elementary stream packet format." Admitted Prior Art does not disclose what format the stream processing unit converts the plurality of data streams.

Yamamoto also does not teach or suggest "wherein the input stream processing unit converts the plurality of data streams to a packetized elementary stream packet format." *Yamamoto* does not contemplate converting the content data before outputting each data stream, much less converting the content data to a packetized elementary stream packet format.

Baxter also does not teach or suggest "wherein the input stream processing unit converts the plurality of data streams to a packetized elementary stream packet format." *Baxter* does not contemplate converting the content data before outputting each data stream, much less converting the content data to a packetized elementary stream packet format.

Thus, Claim 14 has novelty and inventiveness over Admitted Prior Art, *Yamamoto*, and *Baxter*.

With respect to Claim 15, Admitted Prior Art does not teach or suggest "wherein the output stream processing unit modifies a flag in the data stream to reflect that the data stream has been decrypted." The Admitted Prior Art does not mention modifying a flag within the data stream.

Yamamoto also does not teach or suggest "wherein the output stream processing unit modifies a flag in the data stream to reflect that the data stream has been decrypted." *Yamamoto* does not mention modifying a flag within the data stream.

Baxter furthermore does not teach or suggest "wherein the output stream processing unit modifies a flag in the data stream to reflect that the data stream has been decrypted." *Baxter* does not mention modifying a flag within the data stream.

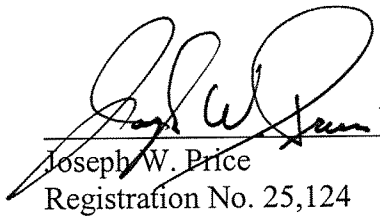
Thus, Claim 15 has novelty and inventiveness over Admitted Prior Art, *Yamamoto*, and *Baxter*.

It is believed that the present claims are allowable over the cited art and an early notice of allowance is requested.

If the Examiner believes a telephone interview will help further the prosecution of this matter, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

Very truly yours,

SNELL & WILMER L.L.P.



Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799